OIPE IAP48
SEP 20 2006
PATENT & TRADEMARK OFFICE

Amendments to the Claims

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1-83. (Canceled)

84. (New) A method of generating a security policy for a predetermined organization, comprising:

receiving a field of business identifier;

receiving an indicator of rigorousness;

retrieving security rules from a stored knowledge base based on the indicator of rigorousness;

generating inquiries regarding the retrieved security rules based upon the field of business identifier and the indicator of rigorousness;

transmitting the generated inquiries to at least one user;

receiving input from the at least one user in response to the transmitted inquiries;

tailoring the retrieved security rules based upon the received input to generate a security policy draft; and

outputting the generated security policy draft that includes the tailored security rules.

85. (New) The method of generating a security policy according to claim 84, wherein transmitting the generated inquiries further comprises transmitting the generated inquiries to members of an organization for review and receiving input further comprises receiving input from the members of the organization.

86. (New) The method of generating a security policy according to claim 85, further comprising generating an information system virtual design based on the received input, the level of rigorousness and the field of business identifier.

87. (New) The method of generating a security policy according to claim 85, further comprising receiving job specifications of the members to receive the inquiries,

wherein generating inquiries includes generating inquiries based upon the field of business identifier, the indicator of rigorousness and the received member job specifications.

88. (New) The method of generating a security policy according to claim 86, wherein receiving input from the members of the organization includes:

storing input received from a member;

comparing input from other members to the stored input;

retransmitting inquiries to members if contradictory inputs are received; and

storing input received from members in response to retransmitted inquiries.

89. (New) The method of generating a security policy according to claim 88, further comprising:

assigning weights to contradictory inputs according to job specifications of the members if contradictory inputs are received from members in response to retransmitted inquiries; and

displaying an estimated response based upon the weighted contradictory inputs.

90. (New) The method of generating a security policy according to claim 88, further comprising:

comparing the information system virtual design and a real information system design and updating the information system virtual design to correct identified differences, thereby obtaining a verified information system virtual design; and

comparing the verified information system virtual design with the generated security policy draft to identify a first set of differences.

91. (New) The method of generating a security policy according to claim 90, further comprising:

assigning priorities to identified differences within the first set of differences; and

generating a schedule for resolving the first set of differences based upon the priorities assigned.

92. (New) The method of generating a security policy according to claim 90, further comprising generating an assessment of a security state of the organization based upon the first set of differences and the received level of rigorousness.

93. (New) The method of generating a security policy according to claim 84, wherein the generated security policy draft includes recommendations for regulations aimed at a specific line of business.

94. (New) The method of generating a security policy according to claim 84, wherein the stored knowledge base includes a set of global guidelines, recommendations or regulations aimed at a specific line of business.

95. (New) The method of generating a security policy according to claim 94, wherein the inquiries are generated based upon the global guidelines.

96. (New) The method of generating a security policy according to claim 84, wherein the stored knowledge base includes security rules related to at least three levels of security policy, including:

executive-level security rules that describe an organization's policy concerning information security, in conformity with global guidelines;

corporate-level security rules that describe an information security system embodying the executive-level information security policy; and

product-level security rules that describe measures for implementing the executive-level security policy with reference to the corporate-level security policy.

97. (New) The method of generating a security policy according to claim 96, wherein the corporate-level security policy includes security rules for the information security system of the overall organization; and includes security rules for individual equipment components constituting the information security system of the organization.

98. (New) The method of generating a security policy according to claim 96, wherein the product-level security policy includes at least two types of product-level security rules, including:

first-level product security rules that describe settings of individual equipment components constituting the information security system in natural language; and

second-level product security rules that describe settings of individual equipment component constituting the information security system in a specific language used in each specific equipment component.

99. (New) An apparatus for generating a security policy for a predetermined organization, comprising:

means for receiving a field of business identifier;

means for receiving an indicator of rigorousness;

means for retrieving security rules from a stored knowledge base based on the indicator of rigorousness;

means for generating inquiries regarding the retrieved security rules based upon the field of business identifier and the indicator of rigorousness;

means for transmitting the generated inquiries to at least one user;

means for receiving input from the at least one user in response to the transmitted inquiries;

means for tailoring the retrieved security rules based upon the received input to generate a security policy draft; and

means for outputting the generated security policy draft that includes the tailored security rules.

100. (New) The apparatus for generating a security policy according to claim 99, wherein the means for transmitting the generated inquiries further comprises means for transmitting the generated inquiries to members of an organization for review and the means for receiving input further comprises means for receiving input from the members of the organization.

101. (New) The apparatus for generating a security policy according to claim 100, further comprising means for generating an information system virtual design based on the received input, the level of rigorousness and the field of business identifier.

102. (New) The apparatus for generating a security policy according to claim 100, further comprising means for receiving job specifications of the members to receive the inquiries,

wherein the means for generating inquiries includes means for generating inquiries based upon the field of business identifier, the indicator of rigorousness and the received member job specifications.

103. (New) The apparatus for generating a security policy according to claim 101, wherein the means for receiving input from the members of the organization includes:

means for storing input received from a member;

means for comparing input from other members to the stored input;

means for retransmitting inquiries to members if contradictory inputs are received; and

means for storing input received from members in response to retransmitted inquiries.

104. (New) The apparatus for generating a security policy according to claim 103, further comprising:

means for assigning weights to contradictory inputs according to job specifications of the members if contradictory inputs are received from members in response to retransmitted inquiries; and

means for displaying an estimated response based upon the weighted contradictory inputs.

105. (New) The apparatus for generating a security policy according to claim 103, further comprising:

means for comparing the information system virtual design and a real information system design and means for updating the information system virtual design to correct identified differences, thereby obtaining a verified information system virtual design; and

means for comparing the verified information system virtual design with the generated security policy draft to identify a first set of differences.

106. (New) The apparatus for generating a security policy according to claim 105, further comprising:

means for assigning priorities to identified differences within the first set of differences; and

means for generating a schedule for resolving the first set of differences based upon the priorities assigned.

107. (New) The apparatus for generating a security policy according to claim 105, further comprising means for generating an assessment of a security state of the organization based upon the first set of differences and the received level of rigorousness.

108. (New) The apparatus for generating a security policy according to claim 99, wherein the generated security policy draft includes recommendations for regulations aimed at a specific line of business.

109. (New) The apparatus for generating a security policy according to claim 99, wherein the stored knowledge base includes a set of global guidelines, recommendations or regulations aimed at a specific line of business.

110. (New) The apparatus for generating a security policy according to claim 109, wherein the inquiries are generated based upon the global guidelines.

111. (New) The apparatus for generating a security policy according to claim 99, wherein the stored knowledge base includes security rules related to at least three levels of security policy, including:

executive-level security rules that describe an organization's policy concerning information security, in conformity with global guidelines;

corporate-level security rules that describe an information security system embodying the executive-level information security policy; and

product-level security rules that describe measures for implementing the executive-level security policy with reference to the corporate-level security policy.

112. (New) The apparatus for generating a security policy according to claim 111, wherein the corporate-level security policy includes security rules for the information security

system of the overall organization; and includes security rules for individual equipment components constituting the information security system of the organization.

113. (New) The apparatus for generating a security policy according to claim 111, wherein the product-level security policy includes at least two types of product-level security rules, including:

first-level product security rules that describe settings of individual equipment components constituting the information security system in natural language; and

second-level product security rules that describe settings of individual equipment components constituting the information security system in a specific language used in each specific equipment component.

114. (New) A storage medium storing a set of program instructions executable on a data processing device and usable for generating a security policy for a predetermined organization, comprising:

instructions for receiving a field of business identifier;

instructions for receiving an indicator of rigorousness;

instructions for retrieving security rules from a stored knowledge base based on the indicator of rigorousness;

instructions for generating inquiries regarding the retrieved security rules based upon the field of business identifier and the indicator of rigorousness;

instructions for transmitting the generated inquiries to at least one user;

instructions for receiving input from the at least one user in response to the transmitted inquiries;

instructions for tailoring the retrieved security rules based upon the received input to generate a security policy draft; and

instructions for outputting the generated security policy draft that includes the tailored security rules.

115. (New) The storage medium according to claim 114, wherein the instructions for transmitting the generated inquiries further comprise instructions for transmitting the generated inquiries to members of an organization for review and instructions for receiving input further comprises receiving input from the members of the organization.

116. (New) The storage medium according to claim 115, further comprising instructions for generating an information system virtual design based on the received input, the level of rigorousness and the field of business identifier.

117. (New) The storage medium according to claim 115, further comprising instructions for receiving job specifications of the members to receive the inquiries,

wherein the instructions for generating inquiries includes instructions for generating inquiries based upon the field of business identifier, the indicator of rigorousness and the received member job specifications.

118. (New) The storage medium according to claim 116, wherein the instructions for receiving input from the members of the organization includes:

instructions for storing input received from a member;

instructions for comparing input from other members to the stored input;

instructions for retransmitting inquiries to members if contradictory inputs are received; and

instructions for storing input received from members in response to retransmitted inquiries.

119. (New) The storage medium according to claim 118, further comprising:

instructions for assigning weights to contradictory inputs according to job specifications of the members if contradictory inputs are received from members in response to retransmitted inquiries; and

instructions for displaying an estimated response based upon the weighted contradictory inputs.

120. (New) The storage medium according to claim 118, further comprising:

instructions for comparing the information system virtual design and a real information system design and updating the information system virtual design to correct identified differences, thereby obtaining a verified information system virtual design; and

instructions for comparing the verified information system virtual design with the generated security policy draft to identify a first set of differences.

121. (New) The storage medium according to claim 120, further comprising:

instructions for assigning priorities to identified differences within the first set of differences; and

instructions for generating a schedule for resolving the first set of differences based upon the priorities assigned.

122. (New) The storage medium according to claim 120, further comprising

instructions for generating an assessment of a security state of the organization based upon the first set of differences and the received level of rigorousness.